# Violencia contra las mujeres en red, vigilancia y el derecho a la privacidad[1]

Florencia Goldsman[2]
Graciela Natansohn[3]

## Resumen

*El objetivo de este trabajo es exponer una reflexión que enlaza la violencia contra las mujeres en entornos digitales, la vigilancia masiva, las discusiones sobre la privacidad y el derecho a la intimidad en internet. Argumentamos que la violencia contra las mujeres (VCM) en ambientes digitales no justifica la vigilancia masiva ni el control extendido sobre los cuerpos y los contenidos relacionados en internet. Para sostener esto examinaremos las diversas nociones de vigilancia y privacidad (Bruno, 2013; Siri, 2015) en relación con el marco civil de internet en función de comprender cómo afectan los derechos humanos de las mujeres en el ciberespacio.*

**Palavras chave**: violencia de género; ciberfeminismos; privacidad; vigilancia; ciberacoso

## 1. Introducción

En este artículo nuestro aporte se centrará en reflexionar acerca de las diversas formas de vigilancia que existen en la actualidad como parte de un *continuum* tecno-político de vigilancias históricas sobre los cuerpos de las mujeres. Las nuevas formas de control se verifican en la actualidad a partir de un entramado, cada vez más complejo, de dispositivos y plataformas digitales que atraviesan nuestras vidas.

Es cierto que el feminismo encontró en la internet una aliada para "hackear el patriarcado" (BOIX, Montserrat, 2016). “El movimiento feminista tiene mucho que ver con

[1] Eixo temático 14 – Privacidade/Vigilância/Controle - IX Simpósio Nacional da ABCiber

[2] Florencia Goldsman é jornalista nacida em Argentina e possui graduação em Comunicación Social pela Universidad de Buenos Aires. Possui 15 anos de trabalho em meios jornalísticos e digitais, revistas e suplementos culturais. Nos últimos anos se especializou em ciberfeminismo e jornalismo com perspectiva de gênero. Seus trabalhos são publicados nos jornal Página 12 (Argentina), Revista Píkara (País Vasco), La Cuerda (Guatemala) e Comunicar Igualdad (Argentina). Atualmente faz mestrado em Comunicação e Cultura na Universidade Federal da Bahia, Brasil, e integra o grupo de pesquisa Gênero, Tecnologias Digitais e Cultura-GIG@, e possui uma bolsa FAPESB. Universidade Federal da Bahia – florcitag@gmail.com

[3] Graciela Natansohn es periodista, magister y doctora en Comunicación, coordina el grupo de investigación Gênero, Tecnologias Digitais e Cultura-GIG@ en Universidade Federal da Bahia, Brasil, donde enseña periodismo, teoria feminista e investiga las posibilidades para una internet feminista. Organizó el libro Internet en código femenino: teorías y prácticas (La Crujía, Argentina, 2013), Jornalismo de Revista em Redes Digitais (Edufba, Brasil, 2013) y es autora de artículos sobre internet, género, mujeres, feminismo y políticas feministas. Universidade Federal da Bahia – graciela71@gmail.com

la forma rizomática de nodos autónomos pero interconectados, con intereses específicos marcados por las diversas agendas pero compartiendo valores y principios comunes", señala Boix (2015, *online*) acerca de la relación entre tecnopolítica y ciberfeminismo. Los nodos difuminados pero también en interconexión a través de las redes adquieren la capacidad de converger en determinados puntos "para lograr tener masa crítica para incorporar la lucha contra el patriarcado a las nuevas dinámicas de cambio que se están generando en todo el planeta. La capacidad colectiva de apropiación de herramientas digitales para la acción colectiva es imprescindible", destaca. Aunque existe una "brecha digital de género" (CASTAÑO, Cecilia, 2008), cuyos orígenes y causas múltiples se relacionan con la posición subordinada de las mujeres en la creación de tecnología, por la educación sexista, por el techo de vidrio en las empresas *high-tech*, por la doble jornada de trabajo y por muchísimas otras causas vinculadas a la histórica subordinación de las mujeres, las cosas están cambiando aceleradamente para las mujeres y las reacciones misóginas no se hacen esperar.

No es por acaso que el tema emergente del activismo feminista contra la violencia de género en Brasil ha sido el fenómeno del odio misógino ejercido mediante y a través de los dispositivos electrónicos com los que interactuamos: internet y dispositivos móviles. En internet, por ejemplo, la violencia contra las mujeres (en adelante, VCM) abarca desde el acoso, hostigamiento, extorsión y amenazas, robo de identidad, *doxxing*[4], alteración y publicación de fotos y videos sin consentimiento. Todos estos ataques afectan de manera real la vida de las mujeres porque generan daño a la reputación, aislamiento, alienación, movilidad limitada, depresión, miedo, ansiedad, trastornos de sueño entre otros[5]. En este contexto surgen, por un lado, reclamos de mayores puniciones, más leyes y más control sobre lo que sucede en internet y por el otro, recaen sobre las mujeres la responsabilidad y, a veces también, la culpa de esas situaciones.

La Asociación para el Progreso de las Comunicaciones (APC) ha recolectado en los últimos seis años más de 1000 relatos de supervivencia y resistencia de mujeres, y alrededor de 2000 incidentes de VCM haciendo uso de espacios en línea y tecnologías de información y comunicación (TIC) están registrados en el mapa mundial de ¡Dominemos la tecnología![6] El propósito de dicho mapa es reunir evidencias para mostrar cómo las TIC pueden usarse para

[4] Significa divulgación de datos personales como domicilio, revelación de datos financieros o teléfonos privados.

[5] Mapa Dominemos la tecnología: https://www.takebackthetech.net/mapit/main?l=es_AR. El propósito de dicho mapa es reunir evidencias para mostrar cómo las TIC pueden usarse para perpetrar violencia contra las mujeres.

[6] https://www.takebackthetech.net/mapit/ Accesado 29/01/ 2017.

perpetrar violencias. Se buscó recolectar información para concientizar y también para que las autoridades y propietarios de las plataformas brinden respuestas y soluciones a la VCM en línea. Otro objetivo fue intentar garantizar un compromiso de los estados para facilitar el acceso de las mujeres a la justicia, cada vez que enfrentan estas violencias. Otro objetivo principal es trabajar con sobrevivientes, activistas contra la VCM y diseñadores/as de políticas para poner fin a la VCM en línea (GENDERIT, 2011).

Amenazas y acciones violentas no son cosa rara: en Brasil diversos personajes que expresan su odio en internet han creado páginas "fake" de conocidas blogueras feministas, divulgando sus datos personales como: teléfono, dirección del domicilio personal como en el caso de la bloguera Lola Aronovich[7], que ha sido amenazada de muerte. A otra bloguera. Ana Freitas, periodista especializada en videojuegos, la acosaron en internet y en su casa: ella y sus vecinos recibían amenazas de muerte por correo y paquetes con todo tipo de cosas desagradables como materia fecal y bichos muertos (GOLDSMAN, Florencia, 2015).

Los derechos a la privacidad, a la libertad de expresión, a decidir libremente y el derecho a la integridad personal están interrelacionados. Así mismo la VCM en ambientes digitales no justifica la vigilancia masiva ni el control extendido sobre internet de manera integral. Muchas y muchos hablan de “una nueva forma de violencia” y sobre la “necesidad de nuevas leyes” cuando se trata de la misma violencia histórica y patriarcal traducida a nuevos formatos y espacios.

Frente a este panorama, el objetivo es exponer una reflexión que considera la tensión entre las posibilidades libertadoras de internet para el movimiento feminista y la expansión de la vigilancia a través de variados dispositivos y usos tecnológicos como una forma de VCM. Este es un tipo de violencia sutil, tanto es así que llega a parecer invisible en la vida cotidiana. Por eso es necesario enlazar la VCM en ambientes digitales y las discusiones sobre privacidad y derecho a la intimidad en internet (BRUNO, Fernanda, 2013; SANTAELLA, Lucia, 2011).

Sostenemos que la VCM en ambientes digitales no justifica la vigilancia masiva ni el control extenso e indiscriminado sobre todo lo que sucede en esas plataformas. Para eso, vamos examinar las diversas nociones de privacidad (SIRI, Laura, 2015; BRUNO, Fernanda, 2013), vigilancia, y algunos ejemplos sobre como las tecnologias móviles y otras

[7] “Meu nome é Lola e estou ameaçada de morte por ser feminista” (Mi nombre es Lola y estoy amenazada de muerte por ser feminista”). Disponible en: http://blogdosakamoto.blogosfera.uol.com.br/2015/11/08/meu-nome-e-lola-e-estou-ameacada-de-morte-por-ser-feminista/ . Accesado 24/01/2016.

biotecnologias pueden ser trampas contra los derechos humanos de las mujeres en el ciberespacio.

## 2. Control sobre los cuerpos y vidas de las mujeres

*“Nunca antes alguien había sido enjuiciado a causa de sus virtualidades mas que de sus actos” Guy Debord, 1967.*

Uno de los síntomas de nuestra época es el hecho de que estamos siendo observados todo el tiempo. “El Estado ha refinado sus instrumentos de vigilancia, y quienquiera huir hacia lo oscuro se enfrentará con artillería iluminadora en su fuga” señalaba el teórico marxista francés Guy Debord ya en los años 60. En la actualidad el flujo de informaciones que circula en el ciberespacio resulta un núcleo privilegiado de monitoramento por parte de diferentes sectores y según diferentes propósitos hacia toda la ciudadanía. Los fines son diferentes: comerciales, publicitarios, administrativos, por motivos de seguridad, afectivos, entre otros. Partiendo desde las diversas formas en que se manifiestan esas nuevas formas de la vigilancia veremos cómo las acciones y comunicaciones cotidianas en el ciberespacio se tornan cada vez más sujetas a colecta, registro, análisis y clasificación.

Por tal razón es necesario colocar de inmediato en el debate cuestiones sobre las implicaciones de estos dispositivos utilizados para la vigilancia, el control y la formación de saberes específicos. En especial aquellos que versan sobre deseos, inclinaciones, conductas y hábitos de individuos y de poblaciones. Es necesario discutir acerca de cómo, sobre las características de la corriente visible de los intercambios y las conversaciones sociales,

> “se constituye un inmenso, distribuido y polivalente sistema de rastreo y categorización de los datos personales que, a su vez, alimenta estrategias de publicidad, seguridad, desarrollo de servicios y aplicativos, dentro y fuera de estas plataformas” (BRUNO, Fernanda, 2013, p. 9)[8] .

Podemos describir los principales aspectos de los procesos de vigilancia en las sociedades contemporáneas conformados a partir de elementos heterogéneos, constituyendo una red multifacetada, repleta de conflictos y ambigüedades. Fernanda Bruno propone la noción de *vigilancia distribuida* como aporte para esta discusión, como una noción operatoria

[8] Original: “Constitui-se um imenso, distribuído e polivalente sistema de rastreamento e categorizaçãode dados pessoais que, por sua vez, alimenta estratégias de publicidade, segurança, desenvolvimento de serviços e aplicativos, dentro e fora destas plataformas” [Todas las traducciones fueron realizadas por las autoras].

más que una definición acabada. Una vía de exploración, entendimiento y problematización que incluye una serie de tensiones en una red en la que interactúan agentes humanos y no humanos. La vigilancia existe como una función potencial que está inscrita en el propio engranaje y arquitectura de esos dispositivos - en el caso de las redes digitales de comunicación como internet y muchas de sus plataformas. Estas, a su vez, contienen, en sus parámetros de funcionamiento regulares, sistemas de monitoramiento de datos personales y control de flujos informacionales que responden a la lógica automatizada de programación que responde a través de protocolos. A su vez los sistemas de monitoreo son parte integrante de la eficiencia de esas plataformas, "que rastrean, archivan y analizan las informaciones disponibilizadas por los usuarios y comunidades de modo de optimizar sus servicios, tanto como las relaciones entre usuarios"[9](BRUNO, Fernanda, op,cit. p. 32). Como afirma Sparrow, "cuando la comunicación es digital, la vigilancia se encuentra justo en su núcleo" (SPARROW, 2014, p.19)[10].

En este contexto, podemos clasificar siguiendo a SPARROW (op.cit) los principales agentes que ejercen acciones de vigilancia en el presente y que abarcan los ámbitos tantos públicos como privados con estrategias distintas, en dos tipos:

a) Estrategia central de modelo de negocios: se manifiesta de diversas formas pero se relaciona con la recolección masiva de datos (minería de datos o *Big Data*) sin el consentimiento de usuarios/as, suscriptores/as a servicios como: apps, redes sociales, servicios de correo, servicios de repositorios de documentos en la "nube". En general se los denomina como "terceros implicados" (*third parties intermediaries*) y centran su estrategia de recolección a través de uso de *cookies* a través de las ventas en línea o del simple seguimiento de la navegación de cada usuario, rastreo de ISPs, respaldos de informaciones, servicios de telefonía, compañías de tarjetas de crédito y cualquier desarrollo de aplicaciones móviles.

b) Estrategia central de seguridad de gobiernos a nivel global: afecta a todxs los ciudadanxs, pero en particular, a activistas, opositores/as y disidentes políticos.

A partir de la comprensión de que las tecnologías y plataformas que usamos cuentan por defecto con algoritmos de monitoreo de las informaciones y acciones de los individuos en

---

9 Original: "Ao contrário, os sistemas de monitoramento são parte integrante tanto da eficiência dessas plataformas, que rastreiam, arquivam e analisam as informações disponibilizadas pelos usuários e comunidadesde modo a otimizar seus serviços, quanto das relações sociais entre os usuários". (traducción nuestra)

10 Original: "When communication is digital, surveillance lies at its very heart". (traducción nuestra)

el ciberespacio, queda claro su modelo de eficiencia (basta pensar en el modo de funcionamiento de cualquier motor de búsqueda). Sin embargo, afirmamos junto con Fernanda Bruno que el hecho de la vigilancia está presente como una posibilidad de la propia arquitectura de esos dispositivos no implica, con todo, que ella sea necesaria. Esto significa que el tener a la mano los datos de navegación, de uso de plataformas ("logueo") y hábitos de la vida virtual de la ciudadanía no debería implicar su sistematización, análisis y uso por fuera de nuestro conocimiento y consentimiento.

La vigilancia a la que nos estamos refiriendo tiene como misión permitirle a quien la ejerce, ya sea desde el ámbito público o desde el privado, la producción de conocimiento sobre los vigilados/as. Aquello que hoy se conoce como "minería de datos"[11] puede ser formalizada de diversas formas (extracción de padrones, regularidades y cadenas causales, por ejemplo). La información cada vez más detallada de quiénes y cómo estamos conectadas/os construyen perfiles minuciosos ("targets") de los usuarios/ consumidores/ciudadanía (ZUAZO, Natalia, 2015, p. 196).

Las actividades de vigilancia enfocadas en individuos o poblaciones humanas involucran, de modo general, tres elementos centrales: observación, conocimiento e intervención (BRUNO, Fernanda, op.cit. p. 18). La observación puede ser efectuada de diferentes modos (visual, mecánico, electrónico, digital) e implica inspección ocular, sistemática y focalizada en individuos, poblaciones, informaciones o procesos comportamentales, corporales y físicos, sociales, entre otros.

Lúcia Santaella (2011) propone tres tipos de regímenes de vigilancia: panóptico, escópico y de rastreamento, aunque los tres operan simultaneamente. El panóptico es el que se realiza en espacios bien circunscritos y fue bien descripto por Michel Foucault en su clásico Vigilar y Castigar, de 1975. El escópico se expresa en la proliferación de cámaras de vigilancia por todos los ámbitos: calles, establecimientos comerciales, edificios y hasta en la intimidad de los domicilios. El de rastreo nace en el espacio digital. Mientras el trabajo de análisis que se precisa hacer del material captado por los sistemas panópticos y escópicos - que requieren procesos de observación, comparación y análisis - el tratamiento de los datos digitales es procesado prácticamente de forma instantánea. Control "ubicuo y pulverizado, de los medios móviles no hay, potencialmente, cómo esconderse. Los lugares son, más bien,

[11] Significado de Minería de datos según Wikipedia, disponible en https://es.wikipedia.org/wiki/Miner%C3%ADa_de_datos . Accesado 22/01/2017.

puntos de un flujo continuo de vigilancia y cada uno de ellos está conectado con otro" (SANTAELLA, Lúcia, 2011, p. 140) [12][traducción nuestra].

Proponemos la tesis de que la vigilancia que aumenta sobre la vida de las personas a través de sus formatos digitales es un tipo de violencia específico que ataca, de forma particular, la libertad de las mujeres para organizarse, expresarse y manifestar su disidencia. En este sentido es preocupante, también, la manera en que la falta de transparencia que ofrecen las plataformas y dispositivos que usamos cada día redunda en un intercambio de datos desigual que resulta en mayor control de cuerpos y voluntades. En el medio de estos intercambios se efectúa la monetización de nuestras informaciones personales y el robustecimiento de unos algoritmos que tiempo después intentarán marcar nuestros hábitos de consumo y preferencias para (¿tal vez?) vendernos productos, remedios o, directamente, un modo de vida.

Gran parte de nuestro comportamiento deja de por sí "huellas digitales" -inclusive de acciones tan inofensivas como viajar en taxi o andar por las calles. "Las cámaras que controlan el tránsito nos monitorean, o nuestros teléfonos celulares registran nuestros paraderos a cada momento del día y nosotros voluntariamente nuestras vidas privadas en plataformas públicas con propietarios privados" (JANE, Fieke, 2014, p.)[13]

Todas las comunicaciones digitales dejan rastro e involucran a terceros implicados (*third-party intermediaries*) entre ellos están proveedores de correo, telefónicas, ISPs, empresas de tarjetas de crédito, ventas en línea, backups físicos o en la *nube* y casi todo desarrollo de apps móviles. "Las redes de los terceros implicados son capaces de rastrear la conducta de los usuarios de internet, incluso cuando los usuarios cambian de dispositivos, porque la mayoría de los sitios web y aplicaciones móviles, usan uno o más de los mismas redes de publicidad" (SPARROW, 2014, p. 24)[14]. Hay que detenerse también, según el mismo autor, en el hecho de que aunque estas redes sean usadas con fines comerciales, las agencias gubernamentales también son capaces de rastrear también esos datos y obtener una rica fuente de datos para vigilancia enfocada en informaciones personales.

[12] Original: "ubíquo e pulverizado, das mídias móveis não há potencialmente como se esconder. Lugares são antes pontos de um fluxo contínuo de vigilância e cada um deles está conectado a outro".

[13] Original: "Traffic and surveillance cameras are monitoring us, our mobile phones ar registering our whereabouts every moment of the day and we voluntarily post our private lives on public proprietary platforms".

[14] Original: "Third-party advertising networks are able to track a user's internet behaviour, even when the user switches devices, because most websites and mobile applications use one or more of the same advertising and tracking networks".

**3. Legislación, vigilancia y (falta de) consentimiento**

El panorama de las tecnologias digitales ha cambiado radicalmente en las últimos décadas. La vigilancia se ha vuelto una "industria comercial, que satisface el interés de los Estados por capacidades de vigilancia cada vez más expansivas. Se calcula que la industria de la vigilancia crece un 20 por ciento al año" (PRIVACY INTERNATIONAL, 2015, p.7). Si bien es cierto que las tecnologías de la vigilancia también tienen como meta brindar protección frente a la amenaza de aumento de la criminalidad en línea, este tipo de desarrollos tecnológicos pueden ser usados por los gobiernos para "hostigar a los detractores, reprimir la disidencia, intimidar a la población, disuadir de ejercer la libertad de expresión y destruir la posibilidad de tener vida privada" (PRIVACY INTERNATIONAL, op.cit., p.7). Shoshana Zuboff (2015) refiere al fenómeno como "capitalismo de la vigilancia".

En junio de 2013 fue revelado un aparato de vigilancia y de espionaje en masa a partir de datos digitales a través de la filtración de copias de documentos de la Agencia de Seguridad Nacional (NSA) de los Estados Unidos de América. La revelación realizada por el hoy perseguido político Edward Snowden[15] señalaba que el programa PRISM permite a la NSA tener acceso directo a servidores de grandes empresas de internet, siendo así capaz de monitorear comportamientos de sus usuarios en escala global. Además, los documentos también detallaron el espionaje a dirigido hacia gobiernos de la diáspora estadounidense, siendo la alta cúpula del gobierno brasilero uno de sus principales focos de atención.

El Marco Civil fue, entonces, una reacción brasilera a la vigilancia en internet. Este documento que pasó por el Senado brasilero el 22 de abril de 2014 y fue sancionado al día siguiente por la hoy depuesta presidenta Dilma Rousseff, lleva el número de ley federal 12965/2014. "Fue el resultado de una amplia movilización de la sociedad civil buscando garantizar los derechos en y de internet – una movilización que resultó en un innovador movimiento de participación en el proceso de creación de leyes brasilero" (ALIMONTI, Veridiana, 2014, p. 83)[16]. Entre los pilares del Marco Civil, que es una ley que está a la vanguardia de los derechos digitales a nivel mundial, se encuentran respeto a la neutralidad, la libertad de expresión, la privacidad y la limitación de la responsabilidad de los intermediarios

[15] "7 mudanças que ocorreram no mundo após as revelações de Snowden". Disponible en: http://www.revistaforum.com.br/2015/06/19/7-mudancas-que-ocorreram-no-mundo-apos-as-revelacoes-de-snowden/. Accesado 22/01/2016.

[16] Original: "which is the result of widespread mobilisation by civil society searching for a guarantee on internet rights – a mobilisation which resulted in an innovative participatory movement in the Brazilian law-making process".

de contenidos como Google, Facebook o Microsoft para filtrar contenidos sin una intervención jurídica previa.

Asi mismo la protección de los datos personales y de la privacidad son, de manera separada, dos de los principios que la ley provee para regular el uso de internet en Brasil. Se marca un punto de inflexión acerca de la conservación de datos de usuarios/as. Vale resaltar que luego de las declaraciones de Snowden, se reforzaron las medidas relativas a la "inviolabilidad y el secreto del flujo de las comunicaciones en la internet y los datos conservados por privados, con la excepción de ser requeridos a través de una orden de la Corte" [17] (ALIMONTI, op.cit., p. 84)[18] en especial en el artículo 7 de esta ley.

Otro de los puntos diferenciales se relaciona con informar a usuarios/as acerca de la recolección de los datos personales por parte de empresas o instituciones.

> La ley requiere consentimiento expreso de parte del sujeto para la futura recolección, uso, conservación y manipulación de los datos personales, que debería ser entregada separadamente de otras cláusulas contractuales (ALIMONTI, op.cit, p. 84).

En otras palabras: se trata de un acceso claro por parte de usuarios/as a la información sobre los procesos que podrían ser realizados con los datos propios, incluyendo la protección en los sistemas de acceso (*log-ins* y *data recording*) a aplicaciones. Siendo éstas últimas fundamentales pues son las de mayor uso, a partir de la expansión del acceso a través de dispositivos móviles. Una cuestión tan sensible como la revelación de datos personales a terceros implicados solo puede ocurrir de existir consentimiento expreso, informado y libre, señala la misma autora.

Como consecuencia del artículo 7, el artículo 8 del Marco Civil declara la garantía del derecho a la privacidad y la libertad de expresión en las comunicaciones como un

---

17 "La inviolabilidad y el secreto de los datos de las comunicaciones son derechos garantizados por la Constitución Federal brasilera, pero el poder judicial entiende que esas provisiones son sólo aplicables al flujo de las comunicaciones y no a las comunicaciones en sí mismas que son guardadas" (ALIMONTI, Veridiana, 2014, p. 84). Original: "The inviolability and secrecy of data and communications are rights guaranteed under the Brazilian Federal Constitution, but the judiciary understands that such provisions are only applicable to the flow of communications, not to communications that are stored". Este detalle es importante debido a las diferenciaciones que se deben hacer entre los datos como contenidos y los **metadatos** como huellas y rastros que deja nuestro paso por la internet.

18 Original: "Such provisions ensure the inviolability and secrecy of the flow of communications on the internet and of stored private data, except if disclosure is required by court order".

prerrequisito y ejercicio de acceso completo a internet[19]. En Brasil, proyectos de ley y agencias reguladoras de las telecomunicaciones vienen intentando instituir medidas que dañen el anonimato en internet. Estas medidas vienen siendo contestadas por sectores de la sociedad civil y de los propios gobiernos, pero aún están en disputa.

Para los casos de VCM en entornos digitales en Brasil existen leyes nacionales y principios legales aplicables, tal como el Código Penal, que caracteriza la injuria, la difamación y calumnia, conocidos como crímenes contra la honra. Amenaza de muerte o violación también están caracterizados en la ley. No hay en el país una ley que caracterice las ofensas y discriminaciones por género como crimen, pues la ley “Maria da Penha” contra la "violencia doméstica" no caracteriza este tipo de daño. A la vez, existen en Brasil diversas iniciativas legislativas para punir los crimes misóginos en red. Pero estos proyectos, específicos para conductas criminales, se enmarcan en una ola vigilantista que reclama el control masivo y general de internet como la única posibilidad de prevenir y enfrentar estos hechos.

En la Argentina, por ejemplo, la Ley 26485 de Protección Integral de la Violencia (2009) si bien no establece mecanismos sancionatorios de la violencia simbólica, en su artículo 5 establece que la “violencia simbólica es la que a través de patrones estereotipados, mensajes, valores, iconos o signos transmite y reproduce dominación, desigualdad y discriminación en las relaciones sociales, naturalizando la subordinación de las mujeres en la sociedad”. En Guatemala, por su parte, la Ley contra la Violencia Sexual, Explotación y Trata de Personas, resulta ser un interesante y oportuno, mecanismo de protección al derecho a la privacidad digital pues (en su artículo 190) establece sanciones para quienes por cualquier medio, sin el consentimiento de la persona, capte mensajes, conversaciones, comunicaciones, sonidos, imágenes en general para afectar la dignidad de su persona (SIERRA-CASTRO, Hedme, 2015).

A finales de 2015 se conformó en la Cámara de Diputados del Brasil una Comisión Parlamentar de Inquérito (CPI) para investigar actividades criminales online. La comisión, conocida como CPICiber, fue escenario de disputas políticas partidarias que poco

[19] “De manera de luchar contra la vigilancia reportada por Snowden, el Artículo 11 determina que la ley brasilera relacionada con privacidad debe ser respetada por quien brinda la conexion a internet y los proveedores de aplicaciones cuando colectan datos personales, *loggeos* y contenidos de las comunicaciones cuando esto ocurra o incluya una terminal localizada em Brasil”. Original: “In order to fight the surveillance reported by Snowden, Article 11 determines that Brazilian law related to privacy must be respected by internet connectivity and applications providers when collecting personal data, logs and communications content when this occurs in the country or involves a terminal located in Brazil”. (ALIMONTI, p. 84).

favorecieron un debate racional sobre la seguridad de las comunicaciones digitales[20]. Las discusiones versaron sobre cómo eliminar contenidos que atentan contra la honra de las personas, los derechos autorales en internet, el acceso indebido a los datos personales de usuarias/os por parte de la policía y el poder judicial, la exigencia de identificación de todos los usuarios/as que accedan sitios web y aplicaciones, con todos los datos de filiación, el bloqueo de aplicaciones y la neutralidad de la red. Todos esos temas se organizaron alrededor de varios proyectos de ley enviados al Congreso por la relatoria de "crímenes contra la honra y otras injurias" de esa CPI, muy criticada por las entidades de la sociedad civil que defienden los derechos humanos en internet por colocar en peligro la libertad de expresión, la privacidad, el acceso. Algunas de esas propuestas constituyen verdaderas amenazas en la medida en que expresan una tendencia al aumento de la vigilancia en nombre de la seguridad de las mujeres[21]. Es imprescindible el anonimato para garantizar el derecho a la libertad de expresión y al disenso político. Para poder profundizar en estos asuntos entendamos ¿qué es la privacidad? y ¿qué tipo de ejercicio de los derechos humanos posibilita?

En el caso de los movimientos de mujeres que luchan por los derechos sexuales y reproductivos es una condición *sinequanon* para poder defender derechos negados. En Chile, como en otros países de la región, la internet se convirtió en una de las plataformas más importantes para que activistas de derechos sexuales y reproductivos expresen sus opiniones, proporcionen información y ejerciten su derecho al aborto. “Pero al mismo tiempo internet invita al acoso y a infringir las normas de privacidad de las comunicaciones” (PEÑA, Paz; BRUNA, Francisca, 2015, p.88).

Existe además un proyecto de ley brasilero que pretende prohibir la producción e intercambio de información sobre aborto, con sentencias de prisión de hasta diez años para quienes incumplan esta norma y brinden ayuda a mujeres que quieran abortar (congressoemfoco.uol.com.br, 2015, en línea). En el caso de profesionales de salud que ayuden a mujeres a abortar sin que las víctimas comprueben haber sufrido violencia sexual podrán ser sancionados con penas de hasta 3 años de prisión de ser aprobado. El Proyecto de Lei nº 5069 de 2013 (PL 5069/2013), cuyo autor es el ex-presidente de la Cámara, Eduardo Cunha (PMDB-RJ) también propone transformar en crimen el “anuncio de medios abortivos”,

[20] Ver: https://antivigilancia.org/pt/2016/09/cpiciber-discurso-de-odio/. Accesado: 30/01/2017.

[21] Disponible: http://www.cartacapital.com.br/blogs/intervozes/cpi-de-crimes-ciberneticos-aprova-relatorio-que-ataca-liberdade-na-internet . Accesado: 30/01/2017.

dificultando la difusión de informaciones sobre los derechos reproductivos y la venta o distribución de métodos contraceptivos[22].

Laura Siri (2015) señala que la privacidad importa por la función social que cumple para permitir la libertad y la democracia. Para ella, el libro “Privacidad Amenazada”, (apud SIRI, 2015) de Helen Nissembaum sirve para entender por qué la privacidad es fundamental:

- La individualidad: porque la oportunidad de un desarrollo personal satisfactorio, creativo y saludable depende en gran parte de la posibilidad de experimentar sin el temor a la desaprobación, censura o el ridículo y sin la presión de adecuarse constantemente a las normas convencionales.

- La autonomía: la privacidad es una manera de mantener la autonomía con respecto a cierta información que una persona considera que no debe ser revelada a terceros.

- Las relaciones sociales: la autonomía de alguien para disponer de los elementos que conforman su vida privada le permite revelar voluntariamente a ciertas personas y en ciertos contextos la información personal que considera oportuna, útil y necesaria.

- La participación política: la privacidad es un valor esencial de todo sistema social y político legítimo. Esconstitutivo de otros derechos tales como la libertad de asociación y de discurso, y sobre todo de la votación secreta sobre la que se funda la democracia.

En este marco, la condición de anonimato se relaciona también con las necesidades de los movimientos de mujeres y personas de las disidencias sexuales.

## 4. Vigilancia sobre los cuerpos de las mujeres

Podríamos afirmar que la historia del cuerpo es la historia de las “panoplias correctivas”[23] (VIGARELLO, 1995), es decir: la trayectoria de un aparato multidisciplinario (dietas, cirugías, deportes, implantes) para modelarlo, domarlo, dominarlo. El movimiento feminista viene discutiendo las formas y definiciones e intervenciones científicas, tecnológicas y médicas del cuerpo de las mujeres que han sido usadas para (re)producir su

[22]Y agrega “El sustitutivo presentado por el relator de la materia en la Comisión de Constituición, Justicia y Ciudadanía (CCJ) de la Câmara, el diputado federal Evandro Gussi (PV-SP), también altera la reciente reglamentación de la atención de personas en situación de violencia sexual y quita la obligación a médicos y enfermeros de informar a las víctimas sus derechos legales y los servicios disponibles”. (traducción nuestra). Disponible: http://congressoemfoco.uol.com.br/noticias/ha-um-conceito-moralista-e-religioso-na-proibicao-do-aborto-legal-diz-deputada/ . Accesado 31/01/2017.

[23] “panóplias corretoras” en el original.

subordinación (NATANSOHN, Graciela, 2005). El ciclo reproductivo se destaca como uno de los principales temas de la biología femenina que parece justificar el macizo desarrollo de tecnologías para su control. La menstruación, la concepción, el parto, el puerperio, las hormonas, la menopausia, la tensión pre-menstrual, todo es objeto de intervención biopolítica. El cuerpo de las mujeres ha sido uno de los pilares sobre los cuales se sustenta la diferencia y subordinación de género y las tecnologías biomédicas han sido actoras principales en el modelaje del cuerpo femenino, sea para controlar, sea para garantizar ideológicamente la perpetuación de su dominación.

Microchips para controlar las dosis hormonales de anticonceptivos hoy substituyen a los todavía novedosos implantes subcutáneos, utilizados también como método de prevención de los embarazos. Si los implantes ponían en cuestión a la falta de autonomía de las mujeres para controlar su funcionamiento, las versiones digitales colocan temas aún más controvertidos. Tal el caso de la empresa Microchips Biotech, Inc., analizado por Daniela Manica (2015), donde un minichip implantado debajo de la piel promete ser activado por una señal de red wi-fi que libera la dosis de droga programada. ¿De qué forma podemos garantizar la seguridad de la administración medicamentosa a distancia? Todavía,

> la posibilidad de que terceros accedan al dispositivo, provocando o inhibiendo la liberación de la substancia sin el control y conocimiento de la usuaria fue relatada como una de las inseguridades del método. También abordamos temas como la necesidad y los límites de una codificación de los datos de los dispositivos móviles que deben controlar los microchips, problematizando la posibilidad de que sean invadidos y controlados por terceras personas, en una especie de hackeamiento ovariano (“ovarian hacking”), inclusive, con eventuales objetivos vengativos (“revenge pregnancy”), como un desdoblamiento similar al que se conoce como pornografía de la venganza (“revenge porn”). (MANICA, Daniela, 2015, online)[24].

En Brasil la colectiva Coding Rights se viene dedicando a estudiar el fenómeno que denominan las “Menstruapps” con el interés de indagar cómo funcionan las aplicaciones para celulares relacionadas con el seguimiento del ciclo menstrual. Estas aplicaciones son

24 Original: “a possibilidade de terceiros acessarem o dispositivo, provocando ou inibindo a liberação da substância sem o controle/ciência da usuária foi levantada como uma das inseguranças do método. Assim, eles abordaram temas como a necessidade, bem como os limites, de uma codificação dos dados dos dispositivos móveis que devem controlar os microchips, problematizando a possibilidade de eles serem invadidos e controlados por terceiros, em uma espécie de hackeamento ovariano (“ovarian hacking”), inclusive com eventuais objetivos vingativos (“revenge pregnancy”), como um desdobramento similar ao que se conhece como pornografia de vingança (“revenge porn”)

ofrecidas para controlar la ovulación, el ciclo y el período fértil, controlar el peso corporal, las medidas del cuerpo (cintura, pecho, caderas), supervisar la presión arterial y el pulso. Algunos calculan el promedio de los últimos ciclos menstruales para predecir la fecha de inicio del próximo, indicar días de fertilidad, ovulación, y períodos actuales y futuros[25].

> Alimentadas con nuestros datos, estas herramientas funcionan como laboratorios para la observación de patrones fisiológicos y de comportamiento, que van desde la frecuencia de la menstruación y los síntomas asociados con ella, hasta los hábitos de compras y navegación por internet de todas sus usuarias. Con las menstruapps, monitorear tu ciclo significa informar regularmente a la aplicación si saliste; bebiste; fumaste; tomaste algún remedio; estabas muy excitada; tuviste sexo; en qué posición estabas cuando tuviste un orgasmo; cómo fue tu caca; si te sentiste triste; si dormiste bien; si tu piel está bien; cómo estás de ánimo; si tu flujo vaginal está más verdoso, tiene mal olor o un aspecto como de crema. (FELIZI, Natasha; VARÓN, Joana. Chupadados, 2016, en línea.)

Uno de los colectores menstruales ofrecidos en el mercado de las "menstruapps" llamado Looncup[26] promete un ciclo menstrual saludable a través de una conexión a dispositivos Android e iOS intermediado por el sistema Bluetooth. Estos sistemas permiten seguir desde el celular el color del flujo y conocer exactamente cuándo es el momento de vaciar y volver a colocar la copa en el interior del canal vaginal. Lo que significa, de alguna manera, dejar en manos del dispositivo la propria percepción del torrente de flujo sanguíneo. Otra propuesta semejante es la de los tampones MyFlow[27], acompañados por un llavero que, combinado con el uso del celular tercerizaría esa acción de auto cuidado tan simple como pasar por el baño para revisar cualquier posible filtración de sangre. Es decir, la mujer le delegaría a su dispositivo el percibir la cantidad de flujo que su cuerpo produce y la decisión de cambiarse o no. En este marco no resulta entonces tan llamativo que las empresas que llevan adelante estas apps, en este caso desde el blog la aplicación Kindara, se animen a publicar "predicciones acerca de la salud de las mujeres en 2016"[28], siendo una de esas proyecciones que "las mujeres confiarán más em sus celulares que en los doctores. En 2016,

25 Algunos ejemplos están disponibles en https://play.google.com/store/apps/details?id=com.woman.diary&hl=es; http://ladytimer.com/ https://www.bebesymas.com/fertilidad/ovuview-aplicacion-movil-para-controlar-el-ciclo-menstrual;https://itunes.apple.com/us/app/my-days-period-ovulation/id470179308?mt=8&at= . Accesado 23/01/2017.

26 Disponible https://tecnoblog.net/186008/looncup-coletor-menstrual-bluetooth/ . Accesado 31/01/2017

27 Disponible: http://www.dailymail.co.uk/sciencetech/article-3595376/A-smart-gadget-far-Online-backlash-against-tampon-uses-bluetooth-tell-wearer-needs-changed.html. Accesado 31/01/2017

28 Disponible: https://www.kindara.com/press-release/2016-predictions . Accesado 31/01/2017

veremos a las mujeres alejándose de los consultorios hacia sus *smartphones*” (Kindara.com. 2016, en línea).

Por el contrario, una búsqueda aleatoria en internet de "aplicativos para hombres"  lleva a recursos y herramientas para medir espacios físicos (reglas, metros, distancias, ángulos), para agendar eventos deportivos, ejercicios físicos para "estar en forma", kit de supervivencia y aplicativos para conocer mujeres, entre otros. Mientras la informatización de los procedimientos clínicos (como la historia clínica de los/las pacientes, por ejemplo) ha sido puesta en debate por las entidades médicas en la medida en que la difusión, manipulación o pérdida y el acceso por personal no autorizado a los datos sanitarios puede acarrear graves consecuencias para el paciente pues vulnera gravemente el derecho a la intimidad y confidencialidad de sus datos médicos. Los aplicativos recogen datos íntimos y los sistematizan “puertas adentro”, es decir; no hacen público para qué esas informaciones pueden ser efectivamente utilzadas cuando las usuarias dan su aprobación a sus términos y condiciones. Y cuándo lo hacen no dejan del todo claro, cuáles son sus posibles consecuencias sobre la salud individual y colectiva. Pero  ¿cómo funcionan esas tecnologías y al servicio de cuales intereses ellas trabajan?

> La cantidad de datos y metadatos recopilados por estas aplicaciones ha posibilitado una cuantificación del cuerpo de las mujeres en una escala nunca antes vista… En momentos en que la privacidad de los datos se ha convertido en unos de los principales temas en debate, estas aplicaciones están recogiendo datos a ritmo veloz y los comparten con terceros que casi siempre permanecen ocultos. (RIZK, Vanessa; OTHMAN, Dalia, 2016, p.15)

La condición de anonimato en internet se relaciona con la información que circula sobre las mujeres: ¿quién la almacena, quién la ve, quién la toca, qué hacen con ella? El anonimato permite la privacidad, que es una forma autonomía y poder. La privacidad y el anonimato empoderan, y son esenciales para determinados contextos políticos, tanto para votar como para asociarse y expresarse. Aún más, el anonimato ha sido uno de los aspectos que más han contribuido para potencializar internet como el espacio cultural, artístico, político y educativo que es hoy.

Al respecto de la gestión y protección de datos personales, la autogestión de la privacidad y el consentimiento relacionado con nuestra información, Daniel Solove (2013) hace una lectura crítica acerca de lo que denomina  “la autogestión de la privacidad”. Para ello se basa en la noción de consentimiento y centra su análisis en si la gente autoriza

determinadas prácticas respecto de su privacidad. En estos casos “el consentimiento legitima casi cualquier tipo de colección, uso o divulgación de datos personales.” Y problematiza que aunque la autogestión de la privacidad sería una posible solución ante cualquier régimen regulatorio, las expectativas puestas en este régimen se encuentran fuera de sus posibilidades. “La autogestión de la privacidad no entrega a las personas un control significativo sobre sus datos. En primer lugar, investigaciones empíricas y de ciencias sociales han demostrado que existen severos problemas cognitivos que socavan la autogestión de la privacidad. Estos problemas cognitivos debilitan la capacidad de los individuos para realizar elecciones informadas y racionales respecto de los costos y beneficios de consentir en la recolección, uso y divulgación de sus datos personales” (SOLOVE, 2013, p.13).

Se trata, también, de detenerse a pensar sobre la digitalización masiva de los ambientes en que vivimos, en estar envueltos en conceptos como "Big Data", "Ciudades inteligentes" e "internet de las cosas", cuyos discursos traen la promesa de que a partir de la abundancia de datos, combinada con la alta capacidad de procesamiento de computadoras con algoritmos inteligentes, brindarán mayor eficiencia tanto en ventas como en la administración pública, así como sobre nuestros cuerpos y hábitos. Fenómeno ante el que debemos parar y preguntarnos ¿hasta dónde estas tecnologías permiten a las mujeres mayor capacidad de agencia y control? O por el contrario ¿aumentan la manipulación de nuestros datos (y cuerpos) sin pedir antes nuestra autorización?

## Conclusiones

Vivimos en un mundo cada vez más “datificado” y según expertas/os en el tema la vigilancia digital aún está en su “infancia” (SPARROW, 2014, GURUMURTHY, 2015). En este contexto de golpes de Estado e intentos de censura a las disidencias políticas es importante contar con un análisis crítico que nos permita estar preparadas para defender nuestros derechos. “En tiempos de crisis políticas, las líneas de comunicación han sido cerradas y las formas críticas de expresión encuentran censura, acoso y arrestos” (JANSEN, 2014, p. 41).

Proyectos de ley brasileros van a contramano de la propia ley del Marco Civil de internet, que está aguardando reglamentación, contrarían uno de los principios más sensibles para los defensores de los derechos a una internet libre, democrática y de acceso universal: “privacidad para el débil, transparencia para el poderoso”.

Delante de este escenario de misoginia y VCM ¿tiene sentido abrir mano del anonimato y de las instancias judiciales para punir criminales? ¿En nombre de quién se va a monitorear, vigilar sin consentimiento y castigar? El panorama actual es contradictorio en Brasil. Por una parte, hay una creciente consciencia y debate público sobre la VCM. Y por otro, una onda conservadora en la política amenaza los derechos humanos básicos, como el derecho a la educación sexual amplia y laica en las escuelas, los derechos reprodutivos de las mujeres, y el derecho a la libertad de expresión a través de las redes.

Las alternativas tecnopolíticas que están siendo discutidas en Brasil, más allá de las características nacionales peculiares, pueden ser extrapoladas al análisis de las tendencias mundiales sobre las políticas de gobernanza para internet que inciden sobre la libertad de expresión, el derecho al disenso y a la privacidad y la situación de los derechos humanos de las mujeres. Hace falta seguir reflexionando y detallando minuciosamente cómo todos estos fenómenos inciden en el caso de la vigilancia como una forma que aumenta la intervención violenta sobre los cuerpos y las decisiones de las las mujeres. Hasta aquí nuestro aporte para continuar el debate.

## Referencias bibliográficas


ALIMONTI, Veridiana. "Marco Civil: A Brazilian reaction to surveillance on the internet" en informe Global Information Society Watch, GISWATCH**,** 2014 - Communications surveillance in the digital age. Disponible en http://giswatch.org/2014-communications-surveillance-digital-age. Accessado en 29/01/2017.

BOIX, Montserrat. "Desde el ciberfeminismo hacia la tecnopolítica feminista". **Pillku** n.18. Año V, setiembre 2015a. Disponible en http://www.pillku.org/article/desde-el-ciberfeminismo-hacia-la-tecnopolitica-fem/ Accesado 24/01/ 2016.

BOIX, Montserrat. Hackeando el patriarcado: La lucha contra la violencia hacia las mujeres como nexo. Filosofía y práctica de Mujeres en Red desde el ciberfeminismo social. **Mujeres en Red**. El periódico feminista. Disponible en http://www.mujeresenred.net/spip.php?article880. Accessado en 29/02/2016.

BRUNO, Fernanda, 2013. **Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade**. Porto Alegre: Sulina, 2013.

CASTAÑO, Cecilia. **La segunda brecha digital**. Madrid: Cátedra/PUV, 2008.

CELE – Centro de estudos em libertad de expresión y acceso a La información. Vargas de Brea Paula, "La regulación de la pornografía no consentida en Argentina", **CELE.** Disponible en http://www.palermo.edu/cele/pdf/Paper-regulacion-pornografia.pdf. Accesado 26/01/2016.

DEBORD, Guy. **La sociedad del espectáculo**. Buenos Aires: La marca editora, 2008.

FELIZI, Natasha; VARÓN, Joana, 2016. "MENSTRUAPPS – ¿Cómo convertir tu menstruación en dinero (para los demás)?" **Chupadados.** Disponible en: https://chupadados.codingrights.org/es/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/ Accesado 24/01/17.

FUNDACIÓN ACCESO. ¿Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección,criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos / Peri, Luciana (coord.). San José, Costa Rica, **Fundación Acceso,** 2015. Disponible en http://acceso.or.cr/files/investigacion-resumen-ejecutivo.pdf Acceso en 29/02/2016.

GENDERIT. "El mapeo como estrategia para develar la violencia contra las mujeres en línea". **GenderIT.** 2011. Disponible en http://www.genderit.org/es/feminist-talk/arma-el-mapa-termina-con-la-violencia-dominemos-la-tecnolog . Accesado 24/01/16.

GENDERIT. *Tweets for women: reflections on challenging misogyny online* . **GenderIT.** 2013. Disponible en: <http://www.genderit.org/feminist-talk/tweets-women-reflections-challenging-misogyny-online>. Accesado en 16/01/16.

GOLDSMAN, Florencia, 2015. "Una internet sin violencia hacia la mujer solo va a suceder em un mundo sin violencia hacia la mujer. **GenderIt, 2015**. Disponible en http://www.genderit.org/es/feminist-talk/una-internet-sin-violencia-hacia-la-mujer-solo-va-suceder-en-un-mundo-sin-violencia-ha . Accesado 30/01/2017.

GURUMURTHY, Anita. "Las mujeres necesitan un nuevo contrato social global, incluyendo la economía digital", 13 diciembre de 2016. disponible en http://www.genderit.org/es/feminist-talk/las-mujeres-necesitan-un-nuevo-contrato-social-global-incluyendo-la-econom-digital. Accesado 03/01/2017

INTERNAUTAS.ORG. "13 principios para el día de la privacidad" Disponible en http://www.internautas.org/html/8764.html . Accesado 25/10/2015. .

JANSEN, Fieke, "From digital threat to digital emergency". Global Information Society Watch, informe Global Information Society Watch, GISWATCH, 2014 - Communications surveillance in the digital age. Disponible en http://giswatch.org/2014-communications-surveillance-digital-age

MANICA, Daniela. SOB A PELE: DE IMPANTELS A CHIPS CONTRACEPTIVOS. In III Simpósio Internacional Lavits, RJ, 2015. Disponible en http://lavitsrio2015.medialabufrj.net/anais/

NATANSOHN, Graciela. O corpo feminino como objeto médico e mediático. **Estudos Feministas,** Florianópolis, 13(2): 256, maio-agosto/2005. Disponível em http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-026X2005000200004

PEÑA, Paz; BRUNA, Francisca. "Fighting the criminalisation of abortion with online information: The case of Aborto Libre" en informe Global Information Society Watch **GISWATCH,** 2015 - Sexual rights and the internet -. Disponible en: https://www.giswatch.org/ar/node/5707 . Diciembre 2015. Acceso 25/10/2016.

PRIVACY INTERNATIONAL. "Demanda y oferta: la industria de la vigilancia al descubierto", 2015.Disponible en https://www.privacyinternational.org/sites/default/files/DemandSupply_Espanol.pdf . Accesado 26/01/2017.

RIZK, Vanessa; OTHMAN, Dalia. Quantifying Fertility and Reproduction through Mobile Apps: A Critical Overview. In: **ARROW PARA EL CAMBIO**. Vol 22, n.1, 2016, pp. 13 a 21. Disponible en http://arrow.org.my/wp-content/uploads/2016/08/AFC22.1-2016.pdf Accesado 26/01/2017.

RUIZ NAVARRO, Catalina. Queridos trolls. 2015. Disponible en http://www.sinembargo.mx/opinion/04-08-2015/37635 . Accesado 26/01/2016.

SANTAELLA, Lucia. As ambivalências das mídias móveis e locativas. In: BEIGUELMAN, Giselle; LA FERLA, Jorge (Org.). **Nomadismos Tecnológicos**. SP: Ed. Senac, 2011, p. 133-149.

SIERRA, CASTRO, Hedme. en FUNDACIÓN ACCESO. ¿Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección,criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos / Peri, Luciana (coord.). San José, Costa Rica, **Fundación Acceso,** 2015. Disponible en http://acceso.or.cr/files/investigacion-resumen-ejecutivo.pdf Acceso en 29/02/2016.

SIRI, Laura. "¿Qué es la privacidad?". Privacidad y vigilancia en entornos digitales. *Curso online de Fundación Vía Libre y Artica*. 2015. Disponible em https://canvas.instructure.com/courses/981219/pages/1-dot-1-que-es-la-privacidad?module_item_id=8288975 Acceso 01/03/2016.

SOLOVE, Daniel, "Autogestión de la privacidad y el dilema del consentimiento", **Revista Chilena de Derecho y Tecnología**, 2013. Disponible en http://comunicacionymedios.uchile.cl/index.php/RCHDT/article/view/30308. Accesado 26/01/2016.

SPARROW, Elijah, "Digital surveillance" en informe Global Information Society Watch **GISWATCH 2014** - Communications surveillance in the digital age. 2014. Disponible en http://giswatch.org/2014-communications-surveillance-digital-age. Acceso 26/01/2016.

VIGARELLO, Georges. Panóplias Corretoras: Balizas para uma história. In: SANT´ANNA, Denise (Org.) **Políticas do corpo.** São Paulo: Estação Liberdade, 1995.

ZUBOFF, Shoshana. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization**. Journal of Information Technology** 30, 2015, p.75–89. Disponible em http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754. Acceso 01/04/2016.

ZUAZO, Natalia, **Guerras de Internet**, Editorial Debate, Argentina, 2015.